# Algebra I

## Musterlösung 14

Zerfällungskörper, endliche Körper

---

**86.** (a) Beweise, dass $(X^2-2X-2)(X^2+1)$ und $X^5-3X^3+X^2-3$ dieselben Zerfällungskörper $K$ über $\mathbb{Q}$ haben, und finde $[K:\mathbb{Q}]$.

(b) Bestimme den Grad eines Zerfällungskörpers des Polynoms $X^3+X^2+1$ über $\mathbb{Q}$ und über $\mathbb{F}_2$.

*Lösung:* (a) Das erste Polynom zerlegt sich über $\mathbb{C}$ in die Linearfaktoren

$$(X^2-2X-2)(X^2+1) = (X-1+\sqrt{3})(X-1-\sqrt{3})(X-i)(X+i).$$

Es besitzt also den Zerfällungskörper $K := \mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{C}$. Das zweite Polynom zerlegt sich zu

$$\begin{aligned} &X^5-3X^3+X^2-3 \\ &\quad = (X^2-3)(X^3+1) \\ &\quad = (X-\sqrt{3})(X+\sqrt{3})(X+1)(X-\tfrac{1}{2}(-1+i\sqrt{3}))(X-\tfrac{1}{2}(-1-i\sqrt{3})). \end{aligned}$$

Es besitzt also den Zerfällungskörper $L := \mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1+i\sqrt{3})) \subseteq \mathbb{C}$. Die Erzeugenden von $L$ sind offenbar in $K$ enthalten, also gilt $L \subseteq K$. Umgekehrt sind wegen

$$i = (2(\frac{1}{2}(-1+i\sqrt{3}))+1)\frac{\sqrt{3}}{3}$$

die Erzeugenden von $K$ in $L$ enthalten, also haben wir $K = L$.

Das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}$ ist $X^2-3$, also gilt $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$. Da $i$ nicht in der reellen Erweiterung $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$ liegt, ist $X^2+1$ das Minimalpolynom von $i$ über $\mathbb{Q}(\sqrt{3})$. Folglich gilt $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] = 2$. Wegen der Multiplikativität des Körpergrades haben wir also

$$[K:\mathbb{Q}] = [K:\mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 4.$$

(b) *Über* $\mathbb{Q}$*:* Das Polynom $f(X) := X^3+X^2+1$ ist ganzzahlig und normiert. Jede rationale Nullstelle ist somit ganz und ein Teiler des konstanten Koeffizienten. Aber $\pm 1$ sind keine Nullstellen; also hat $f$ keine Nullstelle in $\mathbb{Q}$. Wegen $\deg(f) = 3$ ist es deshalb schon irreduzibel über $\mathbb{Q}$.

Da $\deg(f) = 3$ ungerade ist, besitzt $f$ mindestens eine reelle Nullstelle $a$. Um zu untersuchen, ob die anderen beiden Nullstellen ebenfalls in $\mathbb{R}$ liegen, wenden wir Methoden der Analysis an. Die erste Ableitung von $f$ ist $f'(X) = 3X^2+2X = X(3X+2)$; also hat $f$ die beiden lokalen Extrema $f(0) = 1$ und $f(-\frac{2}{3}) = \frac{31}{27}$. Da beide Werte grösser als $0$ sind, kann $f$ keine weitere reelle Nullstelle haben.

Insbesondere liegen die beiden übrigen Nullstellen $b, c \in \mathbb{C}$ von $f$ nicht in $\mathbb{Q}(a)$. Für den Zerfällungskörper $L := \mathbb{Q}(a, b, c)$ von $f$ gilt daher

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(a)] \cdot [\mathbb{Q}(a):\mathbb{Q}] = 2 \cdot 3 = 6.$$

*Über* $\mathbb{F}_2$*:* Durch Einsetzen von 0 und 1 sehen wir, dass $f(X) := X^3+X^2+1$ keine Nullstelle in $\mathbb{F}_2$ hat und somit irreduzibel über $\mathbb{F}_2$ ist. Folglich ist

$$L := \mathbb{F}_2[X]/(X^3 + X^2 + 1)$$

ein Stammkörper von $f$ über $\mathbb{F}_2$. Sei $x \in L$ die Restklasse von $X$. In jedem Körper der Charakteristik 2 ist Quadrieren ein Endomorphismus, insbesondere ist $f(x^2) = f(x)^2 = 0$ in $L$. Wegen $x \neq 0, 1$ gilt andererseits $x^2 \neq x$. Also hat das kubische Polynom $f$ schon die zwei verschiedenen Nullstellen $x, x^2 \in L$; es zerfällt daher bereits über $L$ in Linearfaktoren. Also ist $L$ schon ein Zerfällungskörper von $f$ über $\mathbb{F}_2$. Wegen der Irreduzibilität folgt schliesslich $[L : \mathbb{F}_2] = 3$.

**87.** Konstruiere jeweils einen Zerfällungskörper über $\mathbb{Q}$ für die Polynome $p = X^5 - 1$ und $q = X^4 - 5$ sowie dem Produkt $p \cdot q$. Seien diese Körper $K, L$ und $M$. Beweise:

$$[M : \mathbb{Q}] < [K : \mathbb{Q}] \cdot [L : \mathbb{Q}].$$

*Hinweis*: Beweise mit Hilfe des Schönemann-Eisenstein Kriteriums die Irreduzibilität des Polynoms $X^4 + X^3 + X^2 + X + 1$ über $\mathbb{Q}$.

*Lösung:* Zum Hinweis: Ersetze $X$ durch $X + 1$.

Sei $\mu_5$ eine primitive 5-te Einheitswurzel. Die komplexen Nullstellen von $p$ sind $\mu_5, \mu_5^2, \ldots, \mu_5^5$. Diese sind alle Potenzen von $\mu_5$, daher ist $\mathbb{Q}(\mu_5)$ ein Zerfällungskörper.

Da $X^4 + X^3 + X^2 + X + 1$ irreduzibel und somit das Minimallpolynom von $\mu_5$ ist, folgt $[K : \mathbb{Q}] = 4$.

Die Nullstellen des Polynoms sind $\pm\sqrt[4]{5}, \pm i\sqrt[4]{5}$. Also ist $L = \mathbb{Q}(\sqrt[4]{5}, i)$ ein Zerfällungskörper.

Das Polynom $q$ ist irreduzibel nach Eisenstein mit 5, folglich gilt $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$. Weiters ist $i \notin \mathbb{Q}(\sqrt[4]{5})$, da $i$ nicht reell ist. Daher folgt

$$[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})] \cdot [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Es gilt $M = \mathbb{Q}(\mu_5, i, \sqrt[4]{5})$. Die Erweiterung $M : L$ besitzt höchstens Grad 2, da $\mu_5$ eine Nullstelle des Polynoms $X^2 + \frac{1-\sqrt{5}}{2}X + 1 \in L[X]$ ist. Damit folgt

$$[M : \mathbb{Q}] \leq [M : L] \cdot [L : \mathbb{Q}] \leq 2 \cdot 8 = 16 < [K : \mathbb{Q}] \cdot [L : \mathbb{Q}].$$

**88.** Sei $K$ ein Körper und sei $f \in K[X]$ ein Polynom vom Grad $n \geq 1$. Sei $L$ ein Zerfällungskörper von $f$ über $K$. Beweise:

(a) Es gilt $[L : K] | n!$.

(b) Im Fall $[L : K] = n!$ ist $f$ irreduzibel über $K$.

*Lösung:* (a) Wir verwenden Induktion über $n$. Für $n = 1$ ist $f$ ein lineares Polynom und daher gilt $[L : K] = 1$, woraus die Aussage direkt folgt. Sei also $n \geq 2$. Wir unterscheiden zwei Fälle:

Sei $f$ irreduzibel und $a \in L$ eine Nullstelle von $f$. Dann ist $f$ das Minimalpolynom von $a$ über $K$ und es gilt $[K(a) : K] = n$. Ausserdem lässt sich $f$ über $K(a)$ faktorisieren als $f(X) = (X - a)g(X)$ mit $\deg(g) = n - 1$. Offensichtlich ist $L$ ein Zerfällungskörper von $g$

über $K(a)$. Nach Induktionsvoraussetzung gilt also $[L : K(a)] \,\big|\, \deg(g)! = (n-1)!$. Durch Multiplizieren auf beiden Seiten mit $n$ erhält man

$$[L : K] = [L : K(a)] \cdot [K(a) : K] \,\big|\, (n-1)! \cdot n = n!.$$

Nehmen wir jetzt an, das Polynom $f$ sei reduzibel und seien $f_1, f_2 \in K[X] \backslash K$ mit $f = f_1 f_2$. Dann gilt $n_1 := \deg(f_1) \geq 1$ und $n_2 := \deg(f_2) \geq 1$ und $n = n_1 + n_2$. Sei $K_1$ ein Zerfällungskörper von $f_1$ über $K$. Nach Induktionsvoraussetzung gilt dann für die Erweiterungsgrade $[K_1 : K] \,\big|\, n_1!$. Ausserdem ist $L$ ein Zerfällungskörper von $f_2$ über $K_1$. Nach Induktionsvoraussetzung gilt also $[L : K_1] \,\big|\, n_2!$, und wegen der Multiplikativität des Körpergrades folgt daraus $[L : K] \,\big|\, n_1! n_2!$. Der Binomialkoeffizient $\binom{n_1+n_2}{n_1} = \frac{(n_1+n_2)!}{n_1! n_2!}$ ist eine ganze Zahl, also gilt $n_1! n_2! \,\big|\, (n_1 + n_2)! = n!$. Demnach gilt

$$[L : K] \,\big|\, n!.$$

(b) Da für ein reduzibles $f$ wie oben gilt $[L : K] \,\big|\, n_1! n_2!$ und $n_1! n_2! < n!$, folgt die Aussage.

**89.** (a) Zeige: Das Polynom $h \in K[X]$ ist separabel, wenn $h$ und $D\,h$ keinen gemeinsamen Faktor $\bar{h}$ mit $\operatorname{grad}(\bar{h}) \geq 1$ besitzen.

(b) Zeige: Ist $h \in K[X]$ ein Polynom und besitzen $h$ und $D\,h$ einen gemeinsamen Faktor $\bar{h}$ mit $\operatorname{grad}(\bar{h}) \geq 1$, so ist $h$ nicht notwendigerweise inseparabel.

(c) Zeige: Ist $p$ eine Primzahl, so ist das Polynom $X^{p^n-1} - 1 \in \mathbb{F}_p[X]$ separabel.

*Lösung:* (a) Sei $h$ inseparabel. Sei $g$ ein irreduzibler Faktor von $h$ mit mehrfachen Nullstellen in einem Zerfällungskörper. Dann hat auch $h$ mehrfache Nullstellen in einem Zerfällungskörper. Nach Satz 16.1 haben somit $h$ und $D\,h$ einen gemeinsamen Faktor.

(b) Betrachte das Polynom $p = (X-1)^2$ über einem beliebigen Körper. Es ist niemals inseparabel, da die irreduziblen Faktoren $(X-1)$ einfache Nullstellen haben, aber es hat mit seiner Ableitung $D\,p = 2(X-1)$ einen gemeinsamen Faktor.

(c) Die Ableitung des Polynoms ist $(p^n - 1)X^{p^n-2}$, also eine Potenz des irreduziblen Polynoms $X$. Allerdings ist das Polynom selbst nicht durch $X$ teilbar, hat somit also keinen gemeinsamen Faktor mit seiner Ableitung. Das Resultat folgt nun mit (a).